ProtectUK

Tactic DB5: Cancel or postpone events

ProtectUK publication date
14/12/2023

Information and Intention

Prior to an event being held, a threat, vulnerability and risk assessment (TVRA) specific to the event (and its location) should be used as the basis for determining the protective security requirements and identifying appropriate protective security measures.

The temporary nature of an event may mean that a different mix of security measures may be appropriate compared to a more permanent site. For example, it might be more cost-effective to increase the size of the guard force rather than install more permanent technological solutions. Security measures should be specific to the risks associated with each phase of the event.

If the actual threat or National Threat Level has changed, it may be necessary to cancel or postpone an event.

For incidents involving hostile actors on the ground, further preparation is required. As with other crises, these happen without warning. However, as they often involve public safety, there is further pressure to get things right; understanding how police processes and protocols work is key to planning.

In the event of having to manage a cancellation after the event has started, the communications team should be aligned with operations within the business and key decision makers, from management through to key department heads. The crisis plan must be regularly revisited and tested.

One of the lessons from the Manchester Arena Inquiry was that those in charge of the event did not seem to acknowledge the threat level in their planning process. It is essential that the threat level is considered when planning the measures that may be necessary and proportionate to the event. For further information, view the Purple Guide Chapter on Counter Terrorism – Threat Levels.

Counter Measures:

When developing a proportionate plan for an event, it is essential to understand the principles of protective security. The measures should cover deterring, detecting, delaying, mitigating and responding to an attack. It is not always appropriate to consider all of these aspects but an understanding of how these work together is essential.

- **Deter** involves discouraging adversaries from conducting an attack by making each element appear too physically or technically difficult to achieve. An example of this could be highly visible security patrols around the outside of the event.
- **Detect** involves being alert to potential attack behaviours at every stage, from planning and reconnaissance to deployment. The deployment of behavioural detection operatives or encouraging staff to be aware of hostile reconnaissance behaviour are examples of detection methods.
- **Delay** involves implementing measures that increase the time it takes for attackers to get to the location of vulnerability once the attack starts. This could be ensuring that the right type of perimeter fencing is used to ensure it is harder to penetrate.
- **Mitigate** involves the use of measures to minimise the impact of an attack. The use of a hostile vehicle mitigation system to prevent vehicular access and provide appropriate stand-off is an example of this.
- **Respond** involves ensuring that measures are in place to respond to an incident. This is crucial in ensuring that harm is kept to a minimum. Appropriate training of response staff and a credible response plan are key to ensuring that any incident is dealt with professionally.

Method

It is possible that an event may need to be cancelled or postponed due to an actual threat being present, or due to an increase in risk or vulnerability. This could be as a result of an increase in the National Threat Level (indicating a higher likelihood of attack), or a change in local circumstances.

Threat levels do not have an expiry date and they can change at any time as different information becomes available. This needs to be considered when planning measures. Any plan should be flexible enough to take into account changes in the threat level. This should be reflected in your building response levels.

Building response levels provide a general indication of the protective security measures that should be applied at any given time. There are three types of building response level: Exceptional, Heightened and Normal. A variety of site-specific security measures can be applied in each building response level, although the same measures will not necessarily be found at every location.

Consideration should be given to the practicalities of postponing or cancelling an event where spectators are already at the venue. Some key practical considerations in the case of having to cancel or postpone an actual event taking place include:

- Having a key narrative/message prepared for communication to spectators.
- Maintaining calm and order amongst spectators in the venue.
- Ensuring the rapid, safe, egress of all spectators from the venue.
- Ensuring all staff are aware of their role and ensure this is carried out professionally.
- Securing the venue once it is completely empty.

Private security contractors at events should record lessons learned from event rehearsals, past events or exercises which should then be incorporated into their Standard Operational Procedures (SOPs) for the event. This should include the actions that are required in the case of an event being cancelled or postponed.

Organisations should have a form of words prepared if an event is cancelled or postponed in order to maintain calm and order amongst attendees or spectators. For terrorist-related incidents, reputational damage may be caused if the organisation handles the issue badly, for example communicating insensitively, poorly or not at all.

A crisis communication plan should be a core component of any organisation’s risk preparations. It should be developed following a detailed risk analysis looking at potential issues and possible solutions. Typically, these issues relate to an organisation’s people, assets, property, and operations, and the plan is there to guide action and communications.

It is important that the plan is adapted over time. This should reflect changes in the organisation, new potential risks, updated guidance, and insights gained from test incidents and crises elsewhere. While the course of action will vary for different crises, the principles of the plan will be the same.

Communicating bad news well is now expected of all major organisations. As the result of actions of a hostile actor, the police will have the lead role in communicating to external audiences in an effective and timely fashion. However, the target organisation will remain important and should

reinforce messaging and ensure that consistency and accuracy are maintained. If the police or government department are not the designated point of contact for the media, the organisation should act quickly to take the lead, and position itself as a source of truth.

Dedicated communications channels should be established, with backups, if access to the organisation's intranet or message channels is limited (for example if the network is overloaded, or if it has been the target of the attack). You must provide information for your staff and resources so that they can help deliver the plan.

Event organisers have an obligation under the Health and Safety at Work etc. Act 1974 to provide a safe place for their employees to work, and for the visitors to their attractions and events. Consideration of the risk posed by terrorists must form part of the considerations under this act. It is essential, for corporate governance, to ensure that all threats have been considered and appropriate measures implemented to manage the exposure to risk. It must be recognised and understood that assessing general event risk is different to assessing security risk. It is essential that the person carrying out this task is competent.

Administration

The appropriate policy and procedures should mention the cancellation or postponing of an event and how this is managed. Identify ownership of the responsibility for cancelling an event, what records are kept, and how its effectiveness is assured. For large organisations, there should be a senior manager responsible for the strategic application, and a more junior manager should sit under them who will oversee tactical/operational level issues. For smaller organisations, these roles could be combined and undertaken by one person.

It will be necessary to ensure all staff understand processes and procedures to be adopted, including how to go about reporting suspicious activity or other serious issues.

Risk Assessment

A risk assessment should identify threats which could have an impact on the business, and its vulnerabilities. This risk assessment can be used to define key vulnerabilities or situations and how these should be mitigated against. Risk assessments should clearly define a duty of care to staff and others on both an organisational and individual level. Staff and visitors may have different responses to the same incident and therefore you should risk manage the impact of staff, contractors and/or

visitors, as well as members of the public, not following or directly contradicting instructions.

As identified earlier, a key action for a business is to create a Crisis Communication Plan (TACTIC EB4). This should be a core component of its risk preparations.

Communications

Internal Stakeholder Engagement:

Unless the information is particularly sensitive or involves personal data, all information relating to cancellation or postponement of events should be shared with your staff members. Staff should also be briefed on what to do should they observe suspicious activity at the event, and they should be encouraged to identify and report any suspicious activity or items they observe, or that they know about.

It is necessary to ensure points of contact for the oversight of the event being cancelled or postponed are known to staff internally, and partners externally. Internal communications should encourage security awareness by general staff and a positive security culture should be encouraged through internal communications.

You must provide regular information for your staff so that they can help deliver on the security plan. Your internal audience will inevitably cross over into your external audience, so consider what messages you want them to share with external networks, e.g. families and friends. Remember that social media is a potential area where this crossover may occur.

External Stakeholder Engagement:

Engagement with neighbouring businesses should be on a regular basis and should be constructive. Consideration should be given to the sharing of information regarding cancellation or postponement of an event at your venue, e.g. with transport networks, to remove spectators from the immediate area as quickly as possible where relevant.

Early identification and engagement with key external stakeholders is important. Local organisations whose sites are nearby, or have shared use of the site being protected, are also likely to play an important part in developing and delivering on any security outcomes, and consideration should be given to engaging with any working groups or fora who may already have identified ‘best practices’ and lessons learned from similar sites within the business area the site operates within.

There are a number of key principles that should be applied when engaging with stakeholders:

- The engagement should be different for different stakeholders, at different times – it should be flexible as one type of engagement process does not necessarily suit all stakeholders.
- It should be a two-way engagement process, where information and knowledge are shared.
- Communications should be genuine and timely, where there is the ability to influence outcomes, dependent on feedback.
- Engagement with stakeholders should be open and transparent.

As with all matters relating to security and policing, the relationships with the police are key. The contact may be with either the local police or those specifically tasked with providing policing to certain sites.

Health and Safety/Other Legal Issues

Any actions carried out regarding the communication of information relating to cancellation or postponement of an event may be governed by legislation, such as:

- The Disability Discrimination Act 1995
- The Human Rights Act 1998
- Health and Safety Acts
- The Data Protection Act 2018
- The Fire Safety Order 2005
- The Fire (Scotland) Act 2005

It is important to consider any change to security processes and/or activities with regards to justification, proportionality, necessity and legality.

You should ensure that there are well-defined governance arrangements and that records are kept of the issues, decisions made and the reasoning behind those decisions. Records will provide evidence to any investigations, or public enquiries, and assist in defending against legal action, criminal charges or civil claims. The importance of keeping accurate records and having well defined

governance arrangements has been demonstrated during the Manchester Arena Inquiry.

Such changes that affect visitors, contractors and the organisation must include consideration of relevant legislation as well as details of your organisation’s insurance policies. Consideration must be given regarding the personal health and safety of staff in the performance of their duties, and the general public while they are at your venue.

KEYWORDS
EVENT SECURITY
RISK ASSESSMENT
THREAT
SECURITY MEASURES